



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/764,194	01/17/2001	Fabio Benussi	30990145-US	7542

7590

02/09/2005

Paul D. Greeley
c/o Ohlandt, Greeley, Ruggiero & Perle
Suite 903
One Landmark Square
Stamford, CT 06901

EXAMINER

DADA, BEEMNET W

ART UNIT

PAPER NUMBER

2135

DATE MAILED: 02/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.		Applicant(s)	
	09/764,194		BENUSSI ET AL.	
	Examiner		Art Unit	
	Beemnet W Dada		2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 August 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 2,10-13,17-19,21,23,31,33,35-42,45 and 46 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 2, 10-13, 17-19, 21, 23, 31, 33, 35, 36-42 and 45-46 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This office action is in reply to an amendment filed on August 30, 2004. Claims 21 and 36 have been amended and new claim 46 has been added. Claims 2, 10-13, 17-19, 21, 23, 31, 33, 35, 36-42 and 45-46 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 2, 31, 38, 40, and 45-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slaby et al (hereinafter Slaby), International Publication WO 99121336, in view of Frailong et al (hereinafter Frailong), US Patent 6,073,172.

4. As per claims 45 and 46, Slaby discloses configuring a connectivity unit for communication with a service entity (see for example; router, page 9 ln 21-26), comprising:
Prior to a user taking possession of the unit, pre-installing
configuration communication parameters including an identity-sequence (see for example; page 9 ln 3-16);

Storing user-related information for access by a configuration service (see for example; page 3 In 15-20);

Establishing a connection between the connectivity unit and the configuration service using the configuration communication parameters (see for example; page 8 In 23-page 9 In 3), using the identity-sequence to authenticate the unit to the configuration service (see for example; page 9 In 3-13), and transferring from the service to the unit operational communication parameters including a user-id associating with a user identity derived from said user related information (see for example page 12 In 10-13); and

Subsequently using the operational communication parameters to establish communication between the connectivity unit and service entity (see for example; page 11 In 26-page 12 In 10) with the user-id certificate being used to authenticate the unit to the entity (see for example; page 12 In 10-14). The means of using a user name/password for transmitting to the service provider is well known in the art to serve as a means to authenticate the unit (router) to the service entity.

As for use of certificates linking a public key to an identity sequence and user-id, Slaby further discloses a means of security through encryption (see for example; page 11 In 11-20). Thereby, a means of using encryption (encoding) keys must exist in the system of Slaby. However, Slaby is silent on such means.

Frailong further discloses a means of configuring a connectivity unit through the use of certificates linking a public key of a public-key/private-key cryptographic key pair to an identity (see ifor example; col 18 In 50-65). One of ordinary skill in the art at the time of the applicant's invention would have recognized that such use of certificates for identifying an end-point is advantageous to be used in both the identity sequence of user-id in identifying the connectivity unit. Furthermore, the use of such certificates to identify a user, using their user-id to service

providers is well known in the art. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Frailong within the system of Slaby because it would have provided a means of increased security through the use of trusted certificates for authenticating users/units and further would have allowed for establishing secure communications between peers using well known standards such as Secure Socket Layer.

5. As per claim 2, Slaby-Frailong discloses the claimed limitations above (see claim 45). Slaby further user passing said user-related information to the configuration service (see for example; page 9 ln 3-8). Slaby is silent of the means of purchasing, however many means of purchasing service from a service provider are well known in the art, including the use of a call center. Frailong further discloses a call center for such purchasing means (see for example; col Page 5 ln 12 ln 36-49) and communicating to the call center in one of the following ways: directly by telephone; directly by an electronic messaging system; indirectly through a third party who contacts the call center by telephone; indirectly through a third party who contacts the call center by an electronic messaging system (see for example; col 12 ln 45-59). A call center is inherent in such purchasing means of Frailong to handle such calls, furthermore any means of communication with the call center is well known in the art and just as efficient.

6. As per claim 31, Slaby discloses a configuration service system with a connectivity unit having configuration communications parameters pre-installed therein prior to a user taking possession of the unit (see for example; page 9 ln 3-16), pre-installing configuration communication parameters including an identity-sequence (see for example; page 9 ln 3-16);

A data processing system including a store for holding user-related information (see for example; page 3 ln 15-20);

Art Unit: 2135

Interface means for interfacing the data processing system with the communications infrastructure whereby to enable communication between the data processing system and the connectivity unit of the new user (see for example; page 9 In 8-12); access to the data processing system through the interface means requiring knowledge of at least one said configuration communications parameter (see for example, page 9 In 3-10). Slaby further discloses the data processing system further including; Authentication means comprising means for verifying the authenticity of a said identity-sequence passed by a said connectivity unit to the data processing system across the communications infrastructure (see for example; page 9 In 1-8 and page 11 In 17-21); Means for accessing the user-related information held in said store on the basis of a said identity sequence received from a said connectivity unit in a said identity-sequence authenticated by the authentication means (see for example; page 9 In 10-15), this identity sequence serving to identify the connectivity unit to the data processing system (see for example; page 9 In 3-16); Means for deriving for the connectivity unit of said new user, operational communication parameters on the basis of said user-related information (see for example page 9 In 8-14), these operational parameters including a user associating a user identity derived from said user-related information (see for example; page 12 In 10-14); and Means for transmitting said operational communications parameters to the connectivity unit operational for use by the latter for communicating with said service entity (see for example; page 9 In 8-20 and page 12 In 10-14).

As for use of certificates linking a public key to an identity sequence and user-id, Slaby further discloses a means of security through encryption (see for example; page 11 In 11-20). Thereby, a means of using encryption (encoding) keys must exist in the system of Slaby. However, Slaby is silent on such means. Frailong further discloses a means of configuring a connectivity unit through the use of certificates linking a public key of a public-key/private-key

Art Unit: 2135

Cryptographic key pair to an identity (see for example; col 18 ln 50-65). One of ordinary skill in the art at the time of the applicant's invention would have recognized that such use of certificates for identifying an end-point is advantageous to be used in both the identity sequence of usff-id in identifying the connectivity unit. Furthermore, the use of such certificates to identify a user, using their user-id to service providers is well known in the art. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Frailong within the system of Slaby because it would have provided a means of increased security through the use of trusted certificates for authenticating users/units and further would have allowed for establishing secure communications between peers using well known standards such as Secure Socket Layer.

As for a call center to which user-related information about a new user of a connectivity unit can be passed for entry into the data processing system for storage in said store; the user-related information including the identity sequence of the connectivity unit, Slaby further user passing said user-related information to the configuration service and user related information being established at time of purchase (see for example; page 9 ln 3-8). Slaby is silent of the means of purchasing, however many means of purchasing service from a service provider are well known in the art, including the use of a call center. Frailong further discloses a call center for such purchasing means (see for example; col 12 ln 36-49) and communicating to the call center in one of the following ways: directly by telephone; directly by an electronic messaging system; indirectly through a third party who contacts the call center by telephone; indirectly through a third party who contacts the call center by an electronic messaging system (see for example; col 12 ln 45-59). A call center is inherent in such purchasing means of Frailong to handle such calls, furthermore any means of communication with the call center is well known in the art and just as efficient. Furthermore, in order for authentication of the identity-sequence

such a sequence must be registered to the configuration service for such comparisons as user-related data since each identity sequence is unique to the user.

7. As per claim 38, Slaby discloses a connectivity unit comprising: a store holding configuration communications parameters including an identity-sequence (see for example; page 9 In 3-16); Communication means for establishing communication across said communications infrastructure with a remote entity in accordance with communications parameters held in said store (see for example; page 9 In 3-8), the communications means including authentication means for authenticating the connectivity unit to the remote entity (see for example; page 11 In 11-24), authentication means comprising means for passing a user-identity sequence to the remote entity (see for example; page 11 In 11-24) and Configuration initiation means for causing the communication means to establish communication across said communications infrastructure with a configuration service by using said configuration communications parameters held in said store (see for example; page 9 In 3-8); Download means for downloading operational communications parameters from the configuration service and storing them in said store (see for example; page 9 In 8-20 and page 11 In 20-26); and Operational control means for causing the communication means to establish communication across said communications infrastructure with said service entity by using said operational communications parameters held in said store (see for example; page 9 In 13-20 and page 12 In 1-14); said operational communications parameters including a user-identity linking the identity of a user associated with connectivity unit (see for example; page 12 In 10-15), the user-identity being used by the authentication means for authenticating the connectivity unit to the service entity upon the operational control means causing the communication means to establish communication with the service entity (see for example; page 12 In 10-14). The means

Art Unit: 2135

of using a username/password for transmitting to the service provider is well known in the art to serve as a means to authenticate the unit (router) to the service entity. As for use of certificates linking a public key to an identity sequence and user-id, Slaby further discloses a means of security through encryption (see for example; page 11 ln 11-20). Thereby, a means of using encryption (encoding) keys must exist in the system of Slaby. However, Slaby is silent on such means. Frailong further discloses a means of configuring a connectivity unit through the use of certificates linking a public key of a public-key/private-key cryptographic key pair to an identity (see for example; col 18 ln 50-65). One of ordinary skill in the art at the time of the applicant's invention would have recognized that such use of certificates for identifying an end-point is advantageous to be used in both the identity sequence of user-id in identifying the connectivity unit. Furthermore, the use of such certificates to identify a user, using their user-id to service providers is well known in the art. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Frailong within the system of Slaby because it would have provided a means of increased security through the use of trusted certificates for authenticating users/units and further would have allowed for establishing secure communications between peers using well known standards such as Secure Socket Layer. Furthermore, Frailong discloses use of such certificates for authentication of entities (see for example; col 18 ln 46-54). The use of such certificates for authentication through passing them from one entity to another on a computer network is well known in the art.

8. As per claim 40, Slaby-Frailong discloses the claimed limitations above (see claim 38). Slaby further configuration initiation means responsive to the absence of valid operational communications parameters in said store upon the connectivity unit being powered up and connected to the communications infrastructure (see for example page 18 ln 20-26), to

automatically trigger the communication means to establish communications with the configuration service without requiring the input of data by a user (see for example; page 8 In 26-page 9 In 3 and page 18 In 20-26).

9. Claims 10, 33, and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slaby et al (hereinafter Slaby), International Publication WO 99121336, in view of Frailong et al (hereinafter Frailong), US Patent 6,073,172, and further in view of Carroll, US Patent 6,105,131.

10. As per claims 10 and 33, Slaby-Frailong discloses the claimed limitations above (see claims 45 and 31). As for a cryptographic-based challenge-response interchange conducted between the connectivity unit and configuration service.

Frailong further discloses a means to confirm that the connectivity unit with the public key certificates (see for example; col 18 In 39-45). However, Slaby-Frailong does not explicitly teach a cryptographic-based challenge-response to confirm the connectivity unit is the possessor of the private key related to the public key passed in the identity-sequence certificate whereby to authenticate the unit as the one bearing the identity sequence included in the certificate. Carroll discloses a means of authorizing access to a service (see for example; abstract) and further discloses a means of authentication between two devices through a cryptographic algorithm to confirm the valid possessor of the private key related to a public key (see for example; col 3 In 35-49). The use of such cryptographic-based challenge/response protocol is well known in the art for providing strong authentication of the correct holder of the private key of a certificate. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Carroll within the Slaby-Frailong

combination because it would have increased security by providing an added level of protection on the authenticity of the connectivity unit possessing the public key.

11. As per claim 39, Slaby-Frailong discloses the claimed limitations above (see claim 38).

As for generating and returning a response to a challenge issued by the remote entity, the generation of the response involving the use of said private key to effect a cryptographic operation on data included in the challenge.

This means is well known in the art to be a cryptographic based challenge/response, which is encompassed in claim 10 above and is rejected for the same reasons.

12. Claims 11-13, 17-19, 35, 41, and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slaby et al (hereinafter Slaby), International Publication WO 99/21336, in view of Frailong et al (hereinafter Frailong), US Patent 6,073,172, and further in view of Rigney et al (hereinafter Rigney), Remote Authentication Dial In User Service (RADIUS).

13. As per claim 11, Slaby-Frailong discloses the claimed limitations above (see claim 45). Slaby further discloses a data network to which the configuration service is connected (see for example; frame-relay network, page 8 In 9-26), and an access network to which the user has a subscriber connection (see for example; ISDN network, page 8 In 9-25). As for providing access to the data network through a data-network access point, access points are inherent to such networks in order to provide a connection to the network from a different network and are well known in the art in order to provide translation and forwarding of packets according to different network protocols. The process of establishing a connection between the connectivity unit and the configuration service involving the following sub-steps: The connectivity unit connects via

Art Unit: 2135

the user's subscriber connection access the access network to the data-network access point using addressing information for the latter held as part of said configuration communication parameters (see for example; page 8 In 23-page 9 In 8). Such connection to an access point is well known in the art and is inherent to the means of performing a connection between two different networks using different network protocols. Slaby-Frailong does not explicitly teach the data-network access point authorizing access by the connectivity unit to the data network on the basis of a username and password. Rigney discloses a means of authentication wherein a data-network access point; authorizing access by the connectivity unit to the data network on the basis of a username and password (see for example page 3 paragraphs 1-5) and the data-network access point (network access server) effecting this authorization by using the services of an authorization server associated with the configuration service (RADIUS server; see for example; page 2 introduction-page 3 paragraph 5). As for the username and password being included in said configuration communications parameters and are passed to the access point by the connectivity unit, one of ordinary skill in the art would have recognized such including and passing means to be inherent in such a combination so as to provide the username and password to the network access server for authentication. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Rigney within the Slaby-Frailong combination because it would have promoted security by providing means of authenticating the connectivity unit upon access to the configuration service through a widely used and well known authentication standard. Furthermore, the RADIUS standard is well known in the art to be a means of supporting the management of dispersed serial line and modem pools for large numbers of users, therefore creating the advantage of allowing a configuration service to provide authentication means to large number of users. As for upon access being authorized, the data-network access point assigns an address for the

Art Unit: 2135

connectivity unit of the data network and passes this address to the authorization server which in turn passes it to a configuration manager of the configuration service. Rigney further discloses connecting with client with the service upon authorization, see for example; section 2 pages 4-5). Furthermore, the assigning of an address for the connectivity unit of the data network is to be inherent to Slaby in order for communication to exist between the connectivity unit and other services between the two different networks. Frailong further discloses such address assigning for such communication between a connectivity unit and the data network (see for example col 21 ln 4-11).

As for the configuration manager prompted by the authorization server contacts the connectivity unit at the assigned address of the latter on the data network in order to download said operational communication parameters to the connectivity unit. Slaby discloses an alternative means of such downloading of said operational communication parameters to the connectivity unit wherein the connectivity unit connects to the configuration service (see for example; page 9 ln 3-8) in order to download said operational communication parameters to the connectivity unit (see for example; page 9 ln 3-20). Slaby further discloses a means of downloading operational communication parameters to the connectivity unit wherein a configuration manager contacts the connectivity unit at the assigned address of the latter on the data network in order to download said operational communication parameters to the connectivity unit (see for example; page 12 ln 16-page 13 ln 14). As for the configuration manager being prompted by the authorization server, one of ordinary skill in the art at the time of the applicant's invention would have recognized such a prompting means to be inherent in the Slaby-Frailong-Rigney combination for the means of restricting access before authorization. The means of a configuration manager prompting such download of parameters adds the advantage of reconfiguration or upgrading through the configuration service where the

connectivity unit is not aware of such reconfiguration or upgrading and therefore would not connect to the configuration manager.

14. As per claims 12 and 18, Slaby-Frailong-Rigney discloses the claimed limitations above (see claim 11). Slaby further discloses using the identity sequence as a means of verifying the connectivity unit (see for example; page 9 ln 1-8). The serial number is used to look up the user on the database, therefore, if an incorrect serial number is given, then the connectivity unit is not authenticated. Rigney further discloses the identity sequence of the connectivity unit is in the user name passed to the authorization server (see for example; page 5 paragraph 2) and is checked by the latter against a database of valid identity sequences (see for example; page 5 paragraph 2), access to the data network only being authorized if the identity sequence included in the user name is a valid one (see for example; page 5 paragraph 2).

15. As per claims 13 and 19, Slaby-Frailong-Rigney discloses the claimed limitations above (see claim 11). Rigney further discloses the authorization server being associated with a configuration domain (see for example; page 3 paragraph 2-3, and SMTP address, page 18); the user name passed by the connectivity unit to the data-network access point being of the form: identity sequence of connectivity unit @ configuration domain (see for example; name@fqdn, page 18). As for the data-network access point recognizing the 'configuration domain' as indicating the authorization server to be used thereupon contacting the latter over the data network and passing it the identity sequence contained in the username it received from the connectivity unit. Such recognizing and contacting means are to be inherent to the teachings of Rigney. The identity of multiple servers across different domains (realms) with

'configuration-domain' must be recognized by the data network access point which in managing where the packets are to be sent to in the data network. Without such recognizing, the data access network will not have any means of knowing which authorization server to send such an authentication request.

16. As per claim 17, Slaby-Frailong discloses the claimed limitations above (see claim 45). Slaby further discloses a data network to which the configuration service is connected (see for example; frame-relay network, page 8 ln 9-26), and an access network to which the user has a subscriber connection (see for example; ISDN network, page 8 ln 9-25). As for providing access to the data network through a data-network access point, access points are inherent to such networks in order to provide a connection to the network from a different network and are well known in the art in order to provide translation and forwarding of packets according to different network protocols. The process of establishing a connection between the connectivity unit and the configuration service involving the following sub-steps: The connectivity unit connects via the user's subscriber connection access the access network to the data-network access point using addressing information for the latter held as part of said configuration communication parameters (see for example; page 8 ln 23-page 9 ln 8). Such connection to an access point is well known in the art and is inherent to the means of performing a connection between two different networks using different network protocols. Slaby-Frailong does not explicitly teach the data-network access point authorizing access by the connectivity unit to the data network on the basis of a username and password. Rigney discloses a means of authentication wherein a data-network access point authorizing access by the connectivity unit to the data network on the basis of a username and password (see for example page 3 paragraphs 1-5) and the data-network access point (network access server) effecting this authorization by using the services

Art Unit: 2135

of an authorization server associated with the configuration service (RADIUS server; see for example; page 2 introduction-page 3 paragraph 5). As for the username and password being included in said configuration communications parameters and are passed to the access point by the connectivity unit, one of ordinary skill in the art would have recognized such including and passing means to be inherent in such a combination so as to provide the username and password to the network access server for authentication. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Rigney within the Slaby-Frailong combination because it would have promoted security by providing means of authenticating the connectivity unit upon access to the configuration service through a widely used and well known authentication standard. Furthermore, the RADIUS standard is well known in the art to be a means of supporting the management of dispersed serial line and modem pools for large numbers of users, therefore creating the advantage of allowing a configuration service to provide authentication means to large number of users.

As for upon access being authorized, the data-network access point assigns an address for the connectivity unit of the data network and passes this address to the authorization server which in turn passes it to a configuration manager of the configuration service. Rigney further discloses connecting with client with the service upon authorization, see for example; section 2 pages 4-5). Furthermore, the assigning of an address for the connectivity unit of the data network is to be inherent to Slaby in order for communication to exist between the connectivity unit and other services between the two different networks. Frailong further discloses such address assigning for such communication between a connectivity unit and the data network (see for example col 21 ln 4-11).

As for the data-network access point assigning an address for the connectivity unit on the data network and passing this address to the connectivity unit. Slaby discloses an means of

such downloading of said operational communication parameters to the connectivity unit wherein the connectivity unit connects to the configuration service (see for example; page 9 In 3-8) in order to download said operational communication parameters to the connectivity unit (see for example; page 9 In 3-20). Such communication between two different networks requires the connectivity unit to obtain a network address for the data network in order for connection to the configuration service on the data network. Therefore, the assigning of an address and passing means are to be inherent to Slaby in order for such downloading to exist. Frailong further discloses means of the connectivity unit obtaining the network address from a data network access point (see for example; col 21 In 4-11). As for the addressing and passing upon access being authorized, one of ordinary skill in the art at the time of the applicant's invention would have recognized such addressing and passing means to be inherent in the Slaby-Frailong-Rigney combination for the means of restricting access before authorization. Slaby further discloses the connectivity unit contacting the configuration manager over the data network at an address held by the connectivity unit as part of said configuration parameters (see for example; page 8 In 23-page 9 In 7; the address of the configuration manager must be present in order for such communication to the correct device on a network to exist), the configuration manager subsequently transmitting said operational communication parameters to the connectivity unit (see for example; page 9 In 10-20 and page 1 In 11-page 12 In 5).

17. As per claim 35, Slaby-Frailong discloses the claimed limitations above (see claim 31). Slaby further discloses a data network to which the configuration service is connected (see for example; frame relay network, see for example page 8 In 15-21) and an access network to which the user has a subscriber connection (see for example; ISDN page 8 In 15-21). As for providing access to the data network through a data-network access point, access points are

Art Unit: 2135

inherent to such networks in order to provide a connection to the network from a different network and are well known in the art in order to provide translation and forwarding of packets according to different network protocols. Slaby further discloses the configuration service system having its interface means connected to the data network (see for example; page 8 In 15-21). Slaby-Frailong does not explicitly teach the configuration service further comprising an authorization server for providing a logon authorization service to said data-network access point in respect of connectivity units requesting access to the configuration service system through that access point. Rigney discloses a means of authorizing devices (users) through an authorization server (RADIUS servers) for providing a logon authorization service to a data-network access point (network access server) in respect to users (connectivity units) requesting access to a service (configuration service system) through the access point (network access server; see for example; section 2 pages 4-5). Both Rigney and the Slaby-Frailong combination disclose a means of authenticating users to a service entity would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Rigney within the Slaby-Frailong combination because it would have promoted security by providing means of authenticating the connectivity unit upon access to the configuration service through a widely used and well known authentication standard.

Furthermore, the RADIUS standard is well known in the art to be a means of supporting the management of dispersed serial line and modem pools for large numbers of users, therefore creating the advantage of allowing a configuration service to provide authentication means to large number of users.

18. As per claim 41, Slaby-Frailong discloses the claimed limitations above (see claim 38). Slaby further discloses a data network (see for example; frame-relay network, page 8 In 9-26),

and an access network to which the user has a subscriber connection (see for example; ISDN network, page 8 In 9-25). As for providing access to the data network through a data-network access point, access points are inherent to such networks in order to provide connection to the network from a different network and are well known in the art in order to provide translation and forwarding of packets according to different network protocols. As for said configuration communications parameters held in said store further including the access network address of the data-network access point, Slaby discloses connecting to the data network through the use of configuration communication parameters (see for example; page 9 In 3-7). In order for such connection to be established, the access network address of the data-network access point must be disclosed so as to know where to send access requests. Therefore, such information being in said configuration communications parameters is inherent.

As for providing access through a data-network access point being subject to a username/password authorization process, Slaby-Frailong does not explicitly teach such authorizing using a username/password. Rigney further discloses a username/password authorization process at a data-network access point (network access server), wherein a username and password for use in said authorization process (see for example; section 2 pages 4-5). As for the username including said identity sequence specific to the connectivity unit, Slaby discloses use of such an identity sequence specific to the connectivity unit (see for example; page 11 In 18-21). One of ordinary skill in the art at the time of the applicant's invention would have realized the authentication needing to be done based on the identity sequence (serial number) of the connectivity unit and therefore would have been able to include the identity sequence for use in such username/password authentication.

19. As per claim 42, Slaby-Frailong-Rigney discloses the claimed limitations above (see claim 41). Rigney further discloses the username is of the form: identity sequence of connectivity unit@ configuration domain where the configuration domain serves to indicate to the data-network access point authorization server to be used in the authorization process (see for example; name@fqdn, page 18). As for the data-network access point recognizing the 'configuration domain' as indicating the authorization server to be used thereupon contacting the latter over the data network and passing it the identity sequence contained in the username it received from the connectivity unit. Such recognizing and contacting means are to be inherent to the teachings of Rigney.

The identity of multiple servers across different domains (realms) with 'configuration domain' must be recognized by the data network access point which in managing where the packets are to be sent to in the data network. Without such recognizing, the data access network will not have any means of knowing which authorization server to send such an authentication request.

20. Claims 21, 23, 36, and 37 are rejected under 35 U.S.C. 103(a) as being obvious over Slaby et al (hereinafter Slaby), International Publication WO 99/21336, in view of Frailong et al (hereinafter Frailong), US Patent 6,073,172, and further in view of Zimmerman et al (hereinafter Zimmerman), US Patent 6,526,131.

The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art only under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 103(a) might be overcome by: (1) a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not an invention "by another"; (2) a showing of a date of

Art Unit: 2135

invention for the claimed subject matter of the application which corresponds to subject matter disclosed but not claimed in the reference, prior to the effective U.S. filing date of the reference under 37 CFR 1.131; or (3) an oath or declaration under 37 CFR 1.130 stating that the application and reference are currently owned by the same party and that the inventor named in the application is the prior inventor under 35 U.S.C. 104, together with a terminal disclaimer in accordance with 37 CFR 1.321(c). For applications filed on or after November 29, 1999, this rejection might also be overcome by showing that the subject matter of the reference and the claimed invention were, at the time the invention was made, owned by the same person or subject to an obligation of assignment to the same person. See MPEP § 706.02(1)(1) and § 706.02(1)(2).

21. As per claim 21, Slaby-Frailong discloses the claimed limitations above (see claim 45). Slaby further discloses the connectivity unit seeking to connect to the service entity using the said operational communications parameters to check that the connectivity unit has been correctly configured for communication with the service entity (see for example; 12 In 2-14). Slaby-Frailong is silent on the configuration service initiating the sending of a wake-up indication to the connectivity unit. Zimmerman further discloses sending wake-up indication (see for example; col 1 In 59-col 2 In 6) as being well known in the art. Such wake-up indication means is used to overcome cost differential between outbound and inbound calls to the initiating part (see for example col 1 In 26-35). Furthermore, such wake-up means will allow for the connectivity unit to be disconnected during authorization process, thus relieving the telephone line for other uses until authorization process is completed. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Zimmerman within the Slaby-Frailong combination because it would have provided a means of

Art Unit: 2135

saving money during initialization and further freed up the connection line (telephone line) for other uses during authorization (see for example; col 1 ln 18-35).

22. As per claim 23 and 47, Slaby-Frailong discloses the claimed limitations above (see claims 21 and 36). Slaby further discloses a data network to which the configuration service is connected (see for example: frame relay network, see for example page 8 ln 15-21) and an access network to which the user has a subscriber connection (see for example; ISDN page 8 ln 15-21); and wherein an identifier of the subscriber connection on said access network is stored with said user-related information (see for example page 8 ln 23-page 9 ln 20). As for providing access to the data network through a data-network access point, access points are inherent to such networks in order to provide a connection to the network from a different network and are well known in the art in order to provide translation and forwarding of packets according to different network protocols. Zimmerman further discloses said wake-up indication taking the form of a call placed to said subscriber (see for example; col 1 ln 59-66).

23. As per claim 36, Slaby-Frailong discloses the claimed limitations above (see claim 31). Slaby further discloses the connectivity unit seeking to connect to the service entity after transmitting said operational communication parameter (see for example; 12 ln 2-14). Slaby-Frailong is silent on the configuration service initiating the sending of a wake-up indication to the connectivity unit. Zimmerman further discloses sending wake-up indication (see for example; col 1 ln 59-col 2 ln 6) as being well known in the art. Such wake-up indication means is used to overcome cost differential between outbound and inbound calls to the initiating part (see for example col 1 ln 26-35). Furthermore, such wake-up means will allow for the connectivity unit to be disconnected during authorization process, thus relieving the telephone

line for other uses until authorization process is completed. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Zimmerman within the Slaby-Frailong combination because it would have provided a means of saving money during initialization and further freed up the connection line (telephone line) for other uses during authorization (see for example; col 1 ln 18-35) for other uses during authorization (see for example; col 1 ln 18-35).

As for triggering the wakeup means to send a said wakeup indication to the connectivity unit after the latter has terminated its communication with the data processing system. One of ordinary skill in the art at the time of the applicant's invention would have recognized such means through the combination of Slaby-Frailong and Zimmerman. Such wakeup means must be triggered to initiate such wakeup indication sending. Furthermore, if the connectivity unit hasn't terminated its communication with the data processing system, then such wakeup means is not possible since the connectivity unit is still in connection with another device. Therefore such triggering of wakeup means is to be inherent to the Slaby-Frailong-Zimmerman combination.

Response to Arguments

24. The objection to claim 36 has been withdrawn in view of the amendment filed on August 30, 2004.

25. Applicant's arguments filed August 30, 2004 have been fully considered but they are not persuasive. Applicant argues that Slaby does not teach the step of using the identity-sequence certificate to authenticate the unit to the configuration service. Applicant further argues that

Art Unit: 2135

Slaby does not teach the step of transferring from the service to the unit ... a user-id certificate associating the public key of the unit with a user Identity. Furthermore, applicant argues Frailong does not teach the above noted deficiencies of Slaby. Examiner respectfully disagrees.

Examiner would point out that Slaby discloses establishing a connection between the connectivity unit and the configuration service using the configuration communication parameters (see for example; page 8 ln 23-page! 9 ln 3), using the identity-sequence to authenticate the unit to the configuration service (see for example; page 9 ln 3-13), and transferring from the service to the unit operational communication parameters including a user-id associating with a user identity derived from said user related information (see for example page 12 ln 10-13). Frailong further discloses a means of configuring a connectivity unit through the use of certificates linking a public key of a public-key/private-key cryptographic key pair to an identity (see for example; col 18 ln 50-65). Therefore, the examiner asserts that the combination of Slaby and Frailong teaches the claimed limitations as recited in the claims. Accordingly rejections are respectfully maintained.

Conclusion

26. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

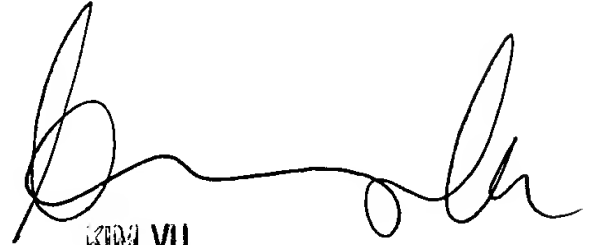
CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada
February 5, 2005



KIM VU
SUPERVISORY PATENT EXAMINER
ELECTRONIC BUSINESS CENTER 2